PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2004-088279

(43) Date of publication of application: 18.03.2004

(51)Int.CI.

9/32 H04L G09C 1/00 HO4H 1/00 H04J 3/00 9/08 HO4L HO4N 7/08 7/081 HO4N HO4N 7/167

(21)Application number: 2002-244570

(71)Applicant: TOSHIBA CORP

(22)Date of filing:

26.08.2002

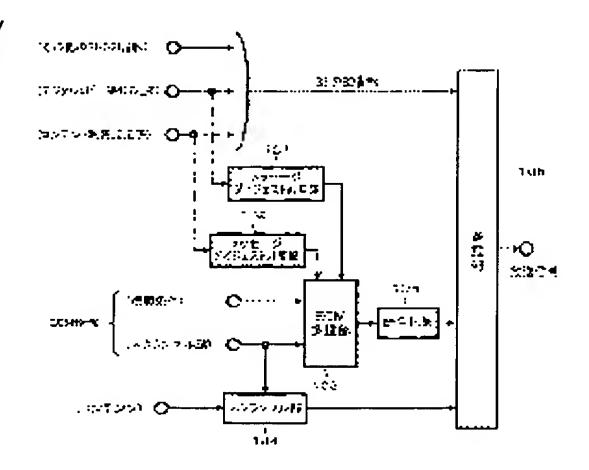
(72)Inventor: OI SHINICHI

(54) BROADCAST TRANSMISSION METHOD AND RECEIVER

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent piracy due to falsified copyright protection information.

SOLUTION: In order to prevent falsification of a digital copy control descriptor and a content utilization descriptor being the copyright protection information, a transmitter side calculates falsification detection data of each descriptor, attaches the data to an ECM and transmits the resulting ECM. A receiver side decides presence / absence of falsification on the basis of received digital copy control descriptor, content utilization descriptor and falsification detection data in the ECM. In the case of decision of the presence of falsification, control of disabled viewing or the like is executed to suppress the falsification thereby protecting the copyright.



LEGAL STATUS

[Date of request for examination]

26.08.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) **日本国特許庁(JP)**

(12) 公 開 特 許 公 報(A)

(11)特許出願公開番号

特開2004-88279 (P2004-88279A)

最終頁に続く

(43) 公開日 平成16年3月18日(2004.3.18)

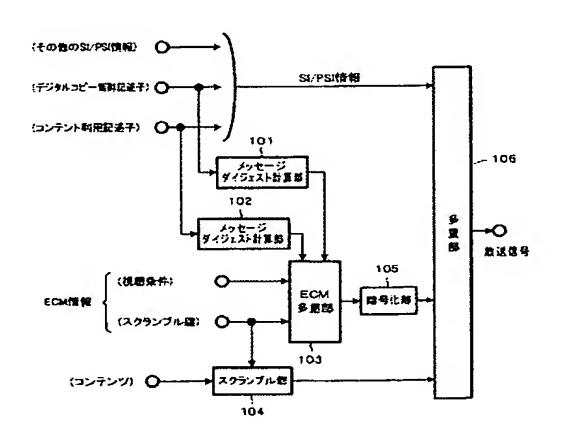
(51) Int.Cl. ⁷		F I					テーマ	マコート	: (参	š)
H04L	9/32	HO4L	9/00	67	75A		5 C (063		
G09C	1/00	G09C	1/00	64	OD		5 C (064		
H 0 4H	1/00	H04H	1/00		В		5 J 🛚	104		
H04J	3/00	HO4H	1/00		${f F}$		5 K (028		
H04L	9/08	HO4 J	3/00		Α					
		審査請求未	水箭	請求項の	D数 6 (O L	(全川	頁)	最終了	真に続く
(21) 出願番号		特顧2002-244570 (P2002-244570)	(71) 出	題人 (0000307	8				
(22) 出題日		平成14年8月26日 (2002.8.26)		4	朱式会社	東芝				
				3	東京都港	区芝浦	一丁目	1番1	号	
			(74)代	理人	0008316	1				
				3	中理士	外川	英明			
			(72) 発	明者	大井 伊·					
				J	東京都青	梅市未	広町2	丁目9	番地	株式会
				7	土東芝青	梅事業	所内			
			Fター	ム (参考	50063	AA01	AB03	AB07	AC01	AC05
						AC10	CA23	CA36	DA07	DA13
						DB10				
					5 C 064	BA01	BB02	BC06	BC17	BC18
						BC22				BD09
						CA14	CB01	CC02	CC04	

(54) 【発明の名称】放送送信方法および受信装置

(57)【要約】

【課題】著作権保護情報の改ざんによる著作権侵害を防止する。

【解決手段】著作権保護用の情報であるデジタルコピー制御記述子およびコンテント利用記述子の改ざんを防止するために、送信側で各記述子の改ざん検出データを計算し、ECMに入れて伝送する。受信側で受信したデジタルコピー制御記述子およびコンテント利用記述子とECM内の改ざん検出データから、改ざんの有無を判定する。改ざんと判定された場合は視聴不可等の制御を行い、改ざんの抑止することで著作権保護が可能となる。



【特許請求の範囲】

【請求項1】

デジタル放送に使用される番組配列情報の一部とされる 著作権保護方式の保護情報であるデジタルコピー制御記 述子およびコンテント利用記述子のうち、少なくとも一 方の前記記述子をスクランブルされた番組とともに送信 する放送送信方法において、

送信される前記記述子が伝送路における改ざんの有無を 受信装置側で検出するために前記記述子から改ざん検出 データを生成し、全受信装置共通の番組のスクランブル を解くための鍵や番組の属性情報を参照する番組情報 (ECM)に多重して暗号化させた情報を、前記スクランブルされた番組ととともに多重させて伝送することを 特徴とする放送送信方法。

【請求項2】

受信側で送信された前記記述子に改ざん有りと検出された場合に、受信側が動作すべき制御方法が規定された改 ざん検出時の制御モード情報をさらに多重させて伝送したことを特徴とする請求項1記載の放送送信方法。

【請求項3】

請求項1に基づいて多重して送信される前記記述子および番組を受信する放送受信装置において、

送信される前記記述子の伝送路における改ざんの有無を 検出し、改ざんがあったと判定された場合は、デスクラ ンブルを不可とする手段を具備むしたことを特徴とする 放送受信装置。

【請求項4】

請求項1に基づいて多重して送信される前記記述子および番組を受信する放送受信装置において、

前記番組のスクランブルを解くデスクランブル手段と、 受信信号に含まれる非暗号化の前記記述子および受信信 号に含まれる全受信装置共通の番組のスクランブルを解 くための鍵や番組の属性情報を参照する番組情報(EC M)とともに暗号化された前記改ざん検出データを計算 した結果とに基づき改ざんを判定する手段と、

前記手段により、改ざんがあったと判定された場合は、 前記デスクランブル手段によるデスクランブルを不可と する制御を行う手段とからなることを特徴とする放送受 信装置。

【請求項5】

請求項2に基づいて多重して送信される前記記述子および番組および改ざん検出時の制御モード情報を受信する 放送受信装置において、

前記番組のスクランブルを解くデスクランブル手段と、 受信信号に含まれる非暗号化の前記記述子および受信信 号に含まれる全受信装置共通の番組のスクランブルを解 くための鍵や番組の属性情報を参照する番組情報(EC M)とともに暗号化された前記改ざん検出データを計算 した結果とに基づき改ざんを判定する手段と、

前記手段により、改ざんがあったと判定された場合は、

改ざん検出時の制御モード情報に従い、受信状態を制御 する手段とを具備することを特徴とする放送受信装置。 【請求項6】

前記ECMからスクランブルされた前記番組をデスクランブルするためのスクランブル鍵を取り出すECM処理手段、前記改ざん検出データを計算する手段、前記改ざんを判定する手段とを少なくともICカード内で処理するものとし、前記デジタルコピー制御記述子もしくはコンテント利用記述子に改ざんがあった場合には、前記ICカードから前記スクランブル鍵を出力しないようにしたことを特徴とする請求項4または5記載の放送受信装置。

【発明の詳細な説明】

[0001]

【発明の属する技術分野】

この発明は、著作権保護方式に対応した放送送信方法および受信装置に関する。

[0002]

【従来の技術】

20 ARIB (社団法人電波産業会)等で規格化検討中の「著作権保護方式」では、番組提供者の権利を保護する 観点から、スクランブルを利用し、番組の権利保護が可 能な受信機のみが復調できるようにしたことにより、放 送された番組の不正な複製を防止することを可能にして いる。

[0003]

具体的には、デジタル放送用受信機等における番組の権利保護を、次の(1)~(3)に記載したように実現している。

- (1) 番組の複製可能な回数等の番組の利用条件を、 番組とともに放送波で伝送する。
- (2) 放送の送り手側は番組等をスクランブルする鍵を管理し、権利保護情報に示す利用条件に従って動作をする受信機に対してその鍵を付与する。
- (3) 受信機から外部接続機器に番組を出力できるのは、その外部接続機器も権利保護情報に示す番組の使用 条件に従う動作をするものである場合に限る。その際、 権利保護情報も付加して出力する。

[0004]

40 ここで、番組の複製可能な回数等の番組の利用条件は、 デジタル放送に使用される番組配列情報(SI(Ser vice Information)、PSI(Pro gram Specific Informatio n))の一部として既に定義もしくは追加定義されるも ので、以下の2つの記述子がそれである。

[0005]

(1) デジタルコピー制御記述子

既に有料放送のための権利保護情報としてARIB標準 規格ARIB STD-B10「デジタル放送に使用す 50 る番組配列情報」に定められている。制約条件なしにコ

ピー可、1世代のみコピー可(受信した放送信号を1回 のみ記録できる)、コピー禁止の3状態を指定可能であ る。

[0006]

(2) コンテント利用記述子

番組配列情報に新たに導入された権利保護情報であり、 コピー禁止の番組に対し、一時的な蓄積の可/不可の指 定と、一時的な蓄積時間の指定(1.5時間、3時間、 ・・・・・、1週間、制限無し)が可能となっている ほか、受信機からデジタルで信号を出力する場合に、暗 10 号化等により出力データを保護するかどうか指定すると いう「出力保護ビット」の指定も可能となっている。

[0007]

しかしながら、規格化検討中の「著作権保護方式」にお けるデジタルコピー制御記述子とコンテント利用記述子 は、非暗号状態で伝送することを前提として規格化が進 んでいる。受信機に入力される前段で上記2つの記述子 が改ざんされた場合には、権利保護情報に示す利用条件 に従って動作する正規の受信機であっても、改ざんされ た記述子の内容に従って動作してしまう。このように今 20 の規格では、不正に対し弱いという欠点がある。

[0008]

【発明が解決しようとする課題】

上記したように、規格化検討中の「著作権保護方式」で は、改ざんされた記述子の内容に従って動作してしまう ことから、このように今の規格では不正に対し弱い、と いう問題がある。

[0009]

この発明の目的は、著作権保護情報に改ざんがあったか どうかで視聴不可の制御を行い著作権保護を図ることに 30 Authentication Code)を計算し、 ある。

[0010]

【課題を解決するための手段】

上記した課題を解決するために、この発明では、著作権 保護情報であるデジタルコピー制御記述子、コンテント 利用記述子の改ざんを防止するために、送信側で保護情 報であるデジタルコピー制御記述子および/またはコン テント利用記述子の改ざん検出データを計算し、番組情 報であるECMに入れて伝送する。受信側では、受信し たデジタルコピー制御記述子、コンテント利用記述子か 40 ら改ざん検出データを計算し、ECM内の改ざん検出デ ータと比較し、改ざんされたかどうかを判定する。

[0011]

上記した手段によれば、著作権保護用の情報であるデジ タルコピー制御記述子、コンテント利用記述子に改ざん があるかどうかを検出し、改ざんがあった場合は視聴不 可等の制御を行い、改ざんの抑止することで著作権保護 が可能となる。

[0012]

【発明の実施の形態】

以下、この発明の実施の形態について、図面を参照しな がら詳細に説明する。図1は、この発明に係る放送側に ついて説明するためのブロック図であり、個別の視聴契 約情報であるEMM(Entitlement Man agement Message)の生成と多重ブロッ クやこの発明に直接に関係のないブロックは省略してあ る。

[0013]

図1において、番組情報配列SI, SPIの情報の一部 として位置付けされる著作権保護方式用の情報であるデ ジタルコピー制御記述子および/またはコンテント利用 記述子は、これ以外の番組配列情報SI、PSIととも に多重部106にて放送信号に多重され放送されるほ か、デジタルコピー制御記述子はメッセージダイジェス ト計算部101にて、コンテント利用記述子はメッセー ジダイジェスト計算部102にて改ざん検出データであ るメッセージダイジェストの計算をそれぞれ行い、全受 信装置共通のECM(Entitlement Con trol Message) とともにECM多重部10 3へ入力される。

[0014]

ここで、ECMは、放送が有料か無料かを表す属性情報 のほか、有料放送である場合には各受信機が予め放送局 から送信され受信し保持しているEMMと比較し、視聴 が可能かどうかを判定するために使用する情報であり、 すなわち番組の視聴条件を示す番組情報である。

[0015]

また、改ざん検出データであるメッセージダイジェスト の具体例としては、送信側でMAC(Message ECMに入れて伝送する。

[0016]

メッセージダイジェストの他の具体例としては、CRC (Cyclic Redundancy Chec k)、パリティー、BCH符号、リード・ソロモン符号 などの秘密情報を使用しない誤り検出可能な符号や、鍵 を使用しないハッシュ関数を利用し生成したものであ る。例えば、放送側で演算したCRCをECMに入れて 伝送する。

[0017]

メッセージダイジェストのもう一つの他の具体例として は、鍵を使用したハッシュ関数やブロック暗号を利用し 生成したものである。使用する鍵は放送局と受信機が予 め秘密裏に共有化しているものとし、例えばECMを暗 号化する際に使用するワーク鍵は予め秘密裏に共有化し ており、また受信機内でもICカードなどのブロック内 に安全に管理されており最適である。ワーク鍵以外に も、放送局と受信機が共有化できている鍵であれば良 い。ここで利用するメッセージダイジェストは秘密の鍵 50 を利用して生成しているものであり、鍵を知らない者が 10

生成する危険性は低いため、放送側で演算したメッセー ジダイジェストを暗号化して伝送する必要は必ずしも無 く、ECM以外の情報として伝送してもよいし、ECM に入れて伝送してもよい。

[0018]

į.

7 . 1 a

図1はメッセージダイジェストの計算に際し鍵を使用し ない場合の例であり、鍵を使用する場合には図示しない 鍵の管理部からメッセージダイジェスト計算部101. 102にそれぞれ鍵が入力されるものである。この場合 の鍵としてECMの暗号化に使用されるワーク鍵を使用 する場合には、暗号部105へ与えられる鍵がメッセー ジダイジェスト計算部101、102にもそれぞれ入力 される。

[0019]

ECM多重部103には、前記メッセージダイジェスト の他に、映像音声データなどの番組のスクランブルに使 用されるECMが多重される。ECM多重部103から 出力されたECMは、暗号化部105にて暗号化され、 多重部106に出力される。

[0020]

なお、暗号化部105で暗号化に使用する鍵をワーク鍵 と呼び、図示しないEMMの生成および管理部で生成保 持し、暗号化部105へ供給されるものである。このワ ーク鍵はセキュリティーの低下を防ぐという目的から、 定期的に例えば1ヶ月に1度という更新周期で更新する ことがあり、更新時には事前に全ての視聴契約者に向け て更新予定の新しいワーク鍵をEMMに入れ送付するよ うになっている。放送局では新しいワーク鍵の入った E MMをほぼすべての受信機が受信した頃を見計らってワ ーク鍵を更新するものである。

[0021]

また、スクランブル部104では映像音声データなどの 番組がスクランクブルされ、多重部16に出力される。 このスクランブルに使用される鍵は、ECMに多重され るスクランブル鍵である。

[0022]

以上説明したように、デジタルコピー制御記述子および コンテント利用記述子のメッセージダイジェストは、E CMに多重された後、暗号化されて受信機まで改ざんさ れることなく伝送可能となる。

[0023]

図2は、この発明の放送受信装置の一実施の形態につい て説明するためのブロック図である。なお、この図2で はEMMの受信部および暗号復号部や、番組配列情報S I. PSIを使用しての番組表生成部や番組表の表示 部、リモコン入力部などユーザーインターフェース部、 などこの発明の説明に直接関係のないブロックは省略し てある。

[0024]

分離部201では、受信した放送信号から番組データ、50【0030】

番組配列情報(SI, PSI)、ECM、図示しないE MMを分離する。分離された番組配列情報 S I, P S I は、さらに分離部203にて番組情報配列SI, SPI の情報の一部であるデジタルコピー制御記述子およびコ ンテント利用記述子、それにこれ以外の番組配列情報S I, PSIに分離される。ここで他の番組配列情報S I, PSIは図示しない番組表生成部で番組表に加工さ れ、オンスクリーン表示などでユーザーに提示したり、 選局時の情報として受信機の制御に使用するものであ る。

[0025]

デジタルコピー制御記述子およびコンテント利用記述子 は著作権保護処理部214に与えられ、著作権保護処理 部214では2つの記述子に従い著作権保護がなされる ように、受信機の出力信号を制御したり、図示しない蓄 積装置において一時的な蓄積が指定時間の間だけできる ように制御したりするものである。また、デジタルコピ ー制御記述子およびコンテント利用記述子はメッセージ ダイジェスト計算部206、207にも与えられ、それ 20 ぞれのメッセージダイジェストを計算する。

[0026]

なお、図2はメッセージダイジェストの計算に際し鍵を 使用しない場合の例であり、鍵を使用する場合には図示 しない鍵の管理部からメッセージダイジェスト計算部2 06,207に鍵がそれぞれ入力されるものである。こ の場合の鍵としてECMの復号化に使用されEMMメモ リ205に記憶されているワーク鍵を使用する場合に は、このワーク鍵がメッセージダイジェスト計算部20 6.207にもそれぞれ与えられる。

30 [0027]

次に、分離部201で分離されたECMは、復号部20 2で暗号の復号を行い、分離部204でメッセージダイ ジェスト、スクランブル鍵、番組に関する視聴条件情報 に分けられる。

[0028]

分離部204で分離された2つの記述子のメッセージダ イジェストはそれぞれ比較部209,210に与えら れ、メッセージダイジェスト計算部206,207でそ れぞれ計算されたメッセージダイジェストと比較判定す 40 る。判定の結果はそれぞれ著作権保護処理部214に与 えられる。

[0029]

分離部204で分離されたスクランブル鍵は、スイッチ 211、スイッチ212を経由して復号部213に与 え、番組の復号が行われる。復号された番組は、図示し ないMPEG (Moving Picture Cod ing Experts Group) でコード処理等 をされた後、著作権保護部214を経由して視聴者に提 供される。

7

分離部204で分離された番組に関する視聴条件情報は、視聴可否判定部208でEMMメモリ205内の個別契約情報と比較判定処理され、視聴可能かどうかの判定を行う。視聴可と判定された場合には、スイッチ211をONし、スクランブル鍵の通過を許可する。

[0031]

14

t a s

著作権保護処理部214では比較部209,210からデジタルコピー制御記述子およびコンテント利用記述子の改ざんの有無が通知され、改ざんがあった場合にスイッチ212をOFFし、スクランブルされた番組の暗号を解くスクランブル鍵をデスクランブル部213に供給しないこととする。従って、出力信号はスクランブルされたままの番組、もしくは出力信号はミュート状態となる。

[0032]

ここで、送信側でMACを計算してECMに入れて伝送した場合は、受信側で受信したデジタルコピー制御記述子およびコンテント利用記述子からMACを計算してECM内のMACと比較し改ざんを判定するためのものである。

[0033]

また、放送側で演算したCRCをECMに入れて伝送した場合、受信側ではECMから取り出したCRCと受信した記述子から計算したCRCとを比較し、両者が一致すれば改ざん無し、不一致なら改ざん有りと判断する。なお放送側で演算したCRCは、暗号で保護されたECMに入れて伝送されるため、このCRC自体が改ざんされる危険性は低い。

[0034]

さらに、鍵を使用したハッシュ関数やブロック暗号を利 30 用して生成したものを E C Mに入れて伝送した場合、受信機では、伝送された改ざん検出データを利用して、デジタルコピー制御記述子およびコンテント利用記述子の改ざんの検出を行う。もし改ざん有りと検出した場合には、 E C Mを使用した視聴可否判定処理によりデスクランブル可(視聴可)であっても、デスクランブル不可とする。

[0035]

図3は、この発明の放送側の他の実施の形態について説明するためのブロック図である。この実施の形態は、図1と比較して改ざん検出時の制御モード情報をECM多重部13に入力し、ECM情報の一部として伝送するところが異なっているのみであるため、以下の説明では、同一の構成部分には同一の符号を付して説明する。

[0036]

改ざん検出時の制御モード情報とは、受信機でデジタルコピー制御記述子またはコンテント利用記述子の改ざん有りと検出した場合に、受信機が動作すべき制御方法を規定したものである。図4に示すように、改ざん検出時の制御モード情報として3ビットをA~Cで定義し、ビ 50

ット1をA、ビット2をB、ビット3をCに対応させて 指定する。

[0037]

すなわち、Aに"1"がたった場合はデスクランブル不可、Bに"1"がたった場合は改ざんのあった記述子の無効化(コピー禁止、または一時蓄積不可)、C"1"がたった場合は、警告のメッセージ表示、A~Cのいずれにも"1"がたたない場合は、何もしない、を切り換えるものである。また、AからCに関しては併用可とするように、改ざん検出時の制御モード情報は、例えばビットマップ指定方式とする。

[0038]

図5を用いてこの発明の放送受信装置の他の実施の形態について説明する。この実施の形態は、図2と比較して図3の送信方法で送信される他の信号とともに多重された改ざん検出時の制御モード情報を、分離部204で分離して著作権保護処理部214に入力する部分、警告メッセージを表示するためのオンスクリーン表示部206の追加した部分が異なっている。また、説明の都合上、20MPEGデコード処理部205も追加している。以下、図2と同一の構成部分には同一の符号を付して説明する。

[0039]

図5において、分離部201では、受信した放送信号から番組データ、番組配列情報(SI, PSI)、ECM、図示しないEMMを分離する。分離された番組配列情報SI, PSIは、さらに分離部203にて番組情報配列SI, SPIの情報の一部であるデジタルコピー制御記述子およびコンテント利用記述子、それにこれ以外の番組配列情報SI, PSIに分離される。ここで他の番組配列情報SI, PSIは図示しない番組表生成部で番組表に加工され、オンスクリーン表示などでユーザーに提示されたり、選局時の情報として受信機の制御に使用するものである。

[0040]

デジタルコピー制御記述子およびコンテント利用記述子は著作権保護処理部214に与えられ、著作権保護処理部214では2つの記述子に従い著作権保護がなされるように、受信機の出力信号を制御したり、図示しない蓄積装置において一時的な蓄積が指定時間の間だけできるように制御したりするものである。またデジタルコピー制御記述子およびコンテント利用記述子はメッセージダイジェスト計算部206,207にも与えられ、それぞれのメッセージダイジェストを計算する。

[0041]

なお、図5はメッセージダイジェストの計算に際し鍵を使用しない場合の例であり、鍵を使用する場合には図示しない鍵の管理部からメッセージダイジェスト計算部206,207に鍵がそれぞれ入力されるものである。この場合の鍵としてECMの復号化に使用されEMMメモ

リ25に記憶しているワーク鍵を使用する場合には、こ のワーク鍵がメッセージダイジェスト計算部206,2 07にもそれぞれ与えられる。

[0042]

A Commence

次に、分離部201で分離されたECMは復号部202 で復号され、分離部204でメッセージダイジェスト、 改ざん検出時の制御モード情報、スクランブル鍵、番組 に関する視聴条件情報に分けられる。分離部204で分 離された2つの記述子のメッセージダイジェストは、比 較部209.210にそれぞれ与えられ、メッセージダ 10 イジェスト計算部206、207でそれぞれ計算された メッセージダイジェストと比較判定する。判定の結果は それぞれ著作権保護処理部214に与えられる。

[0043]

分離部204で分離されたスクランブル鍵は、スイッチ 211.212を経由して番組のデスクランブル部21 3に与えられ、デスクランブルされた番組は、MPEG デコード処理部215でデコード処理等をされた後、オ ンスクリーン表示部216および著作権保護部214を 経由して視聴者に提供される。

[0044]

分離部204で分離された番組に関する視聴条件情報 は、視聴可否判定部208でEMMメモリ205内の個 別契約情報と比較判定処理され、視聴可能かどうかの判 定を行う。判定の結果視聴可と判定した場合には、スイ ッチ211をONし、スクランブル鍵の通過を許可す る。

[0045]

著作権保護処理部214では比較部209,210から デジタルコピー制御記述子およびコンテント利用記述子 30 以上説明したように、著作権保護方式に関わるデジタル の改ざんの有無が通知され、改ざんがあった場合には、 分離部204から入力される改ざん検出時の制御モード 情報に従い受信機を制御する。

[0046]

なお、改ざん検出時の制御モード情報は、図4に示すよ うに、改ざん検出時の制御モード情報として3ビットを A~Cで定義し、ビット1をA、ビット2をB、ビット 3をCに対応させて指定する。

[0047]

すなわち、デスクランブル不可の場合には、著作権保護 40 処理部214はスイッチ212をOFFし、スクランブ ル鍵を番組のデスクランブル部213に供給しないこと とする。従って、出力信号はスクランブルされたままの 番組となる。

[0048]

警告のメッセージ表示の場合には、著作権保護処理部2 14はオンスクリーン表示部216に対し警告のメッセ ージ表示を行うように制御する。なお、警告メッセージ は固定的なメッセージとして著作権保護処理部214で 予め製造時等に記憶しておき、著作権保護処理部214 50 以上説明したように、この発明によれば、著作権保護用

に対しデータ提示しても良いし、番組配列情報 S I, P SIの一部として放送側から提供されたものを、分離部

203で分離し使用しても良いものとする。

[0049]

改ざんのあった記述子の無効化の場合には、著作権保護 処理部214は改ざんのあった記述子の無効化を行うよ うに動作する。すなわち、デジタルコピー制御記述子に 改ざんがあった場合には出力信号をコピー禁止の制御を した上で出力するものである。また、コンテント利用記 述子に改ざんがあった場合には、図示しない蓄積装置に 対し番組の一時蓄積を不可とする制御を行うものであ る。

10

[0050]

以上説明した例では、メッセージダイジェストをECM 内で伝送する例であったが、メッセージダイジェストを ワーク鍵等の暗号鍵を使用し計算するものとすればEC M内で伝送する必要はない。その場合には、暗号鍵を管 理している管理部、例えば受信機に使用されるICカー ドなどでデジタルコピー制御記述子もしくはコンテント 20 利用記述子からメッセージダイジェストの計算を行うこ ととし、暗号鍵が公開されないようにするものとする。

[0051]

そしてICカードにはECMを処理し、契約がある場合 にはスクランブル鍵が出力される処理とともに、前記メ ッセージダイジェストの計算結果と、伝送されたメッセ ージダイジェストの比較を行い、改ざんがあった場合に はICカードから前記スクランブル鍵の出力を行わない 等の処理をするものである。

[0052]

コピー制御記述子またはコンテント利用記述子の改ざん 検出をすることにより、両記述子の改ざんを検出するこ とができ、改ざんがあった場合には視聴不可等の制御を することで改ざんの抑止することができる。

[0053]

また、改ざん検出用のメッセージダイジェストは、スク ランブル鍵とともに E C M内で暗号化され伝送されるた め、メッセージダイジェスト自体の改ざんがされること なく安全に受信機に伝送されるほか、スクランブル鍵の 管理と平行して改ざんの有無を検出するため、改ざんが あった場合には視聴不可等の制御をすることも可能とな る。

[0054]

さらには改ざんが検出された場合の受信機制御の方法を 複数種類設け、放送波で制御可能とすることにより、改 ざんがあった場合のペナルティーのレベルを切り換える ことが可能となる。

[0055]

【発明の効果】

(7)

II

の情報であるデジタルコピー制御記述子およびコンテン ト利用記述子に改ざんがあるかを検出し、改ざんが検出 された場合は視聴不可等の制御を行い、改ざんを抑止す ることが可能となる。

【図面の簡単な説明】

【図1】この発明の送信側の一実施の形態について説明 するためのブロック図。

【図2】この発明の受信側の一実施の形態について説明 するためのブロック図。

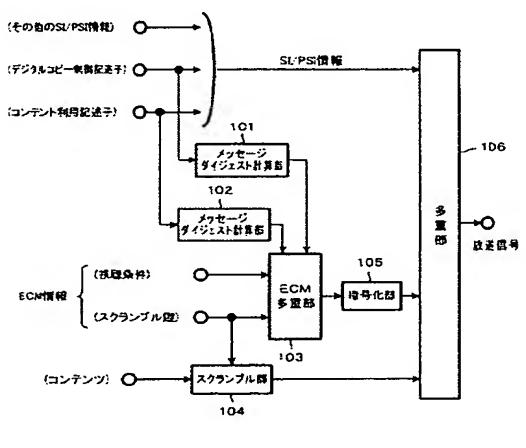
【図3】この発明の送信側の他の実施の形態について説 10 205・・・EMMメモリ 明するためのブロック図。

【図4】この発明の改ざん検出時の制御内容について説 明するための説明図。

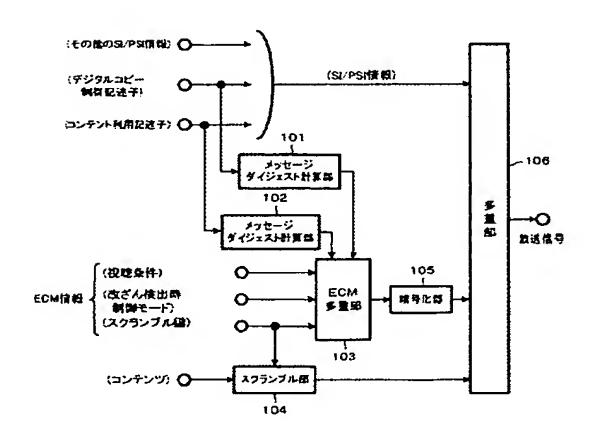
【図5】この発明の受信側の他の実施の形態について説 明するためのブロック図。

【符号の説明】

【図1】



【図3】



12 101, 102, 206, 207・・・メッセージダイ

ジェスト計算部

103・・・ECM多重部

104・・・スクランブル部

105・・・暗号化部

106・・・多重部

201, 203, 204 · · · 分離部

202・・・復号部

213・・・デスクランブル部

208・・・視聴可否判定部

209, 210・・・比較部

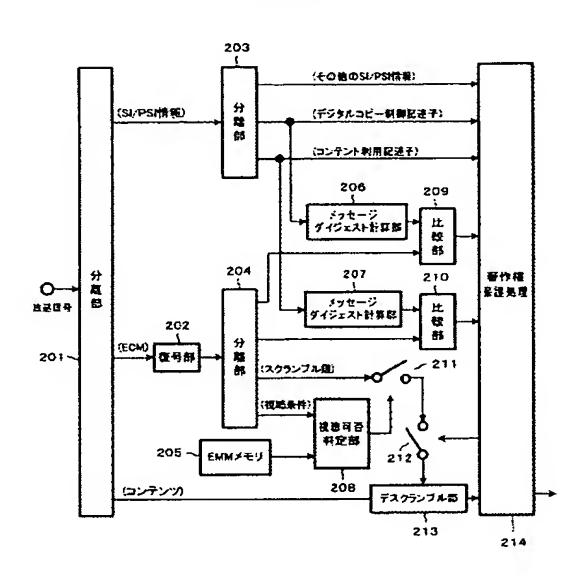
211, 212 · · · スイッチ

214・・・著作権保護処理部

215··・MPEGデコード処理部

216・・・オンスクリーン表示部

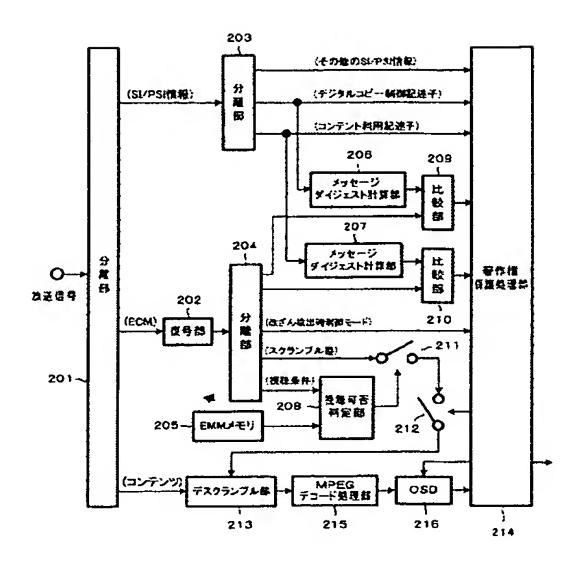
【図2】



【図4】

ビット			改ざん後出時の制製内容				
A	8	С	体にいる田崎の創設とは				
0	0	0	何もしない				
1	0	0	デスクランブル不可				
0	1	0	改ざんのあった記述子の無効化(コピー禁止、または一時皆様不可)				
0	0	1	芸告のメッセージ表示				
1	1	0	デスクランブル不可、改ざんのあった記述子の療効化(コピー禁止、 または一時習得不可)				
1	0	1	デスクランブル不可、勧告のメッセージ表示				
0	1	1	改ざんのあった記述子の無効化(コピー禁止、または一時間積不可) 警告のメッセージ表示				
1	1	1	デスクランブル不可、改ざんのあった記述子の無効化(コピー禁止、 または一時表表不可)、各合のメッセージ表示				

【図5】



フロントページの続き

(51) Int. CI. ⁷			FI			テーマコード(参考)
H O 4 N	7/08		H 0 4 N	7/08	Z	
H O 4 N	7/081		H 0 4 N	7/167	Z	
H O 4 N	7/167		H O 4 L	9/00	6 0 1 B	
F ターム (参考	5J104 AA08	AA12 AA13	LA01 LA02 L	A05 NA02	NA35 PA05	
	5K028 EE05	KK01 KK03	KK12			